Amendments to the CLAIMS:

Without prejudice, this listing of the claims replaces all prior versions and listings of the claims in the present application:

LISTING OF CLAIMS:

1-10. (Canceled).

11. (Currently Amended) A method for transmitting signals between a transmitter and a receiver, the method comprising:

calculating data as a function of a secret key using at least one cryptographic algorithm in a calculation phase; and

calculating authentication tokens for the signals as a function of the data in a communication phase so as to authenticate both the signals and a transmission sequence of the signals;

wherein the signals received by the receiver from the transmitter are accepted as authentic if a transmitted authentication token that is received by the receiver matches the authentication token calculated by the receiver.

12. (Previously Presented) The method as recited in claim 11 wherein the calculation phase includes generating a pseudo-random sequence.

13. (Previously Presented) The method as recited in claim 12 wherein certain strings of the pseudo-random sequence are used for coding the signals and positions in the transmission sequence, and wherein the authentication token of one of the signals transmitted at an i-th position is calculated as a function of the coding of the signal and the coding of the respective position in the transmission sequence.

14. (Previously Presented) The method as recited in claim 13 wherein the authentication token of the one signal transmitted at the i-th position is a bit-by-bit XOR link or an equivalent logic function of the coding of the one signal and the coding of the respective position in the transmission sequence.

15. (Previously Presented) The method as recited in claim 11 wherein the calculation phase includes generating a pseudo-random sequence.

16. (Previously Presented) The method as recited in claim 15 wherein certain strings of the pseudo-random sequence are used for coding the signals and positions in the transmission sequence, and wherein the authentication token of a one of the signals transmitted at an i-th position is calculated as a function of the coding of all previously transmitted signals and the coding of the respective position in the transmission sequence.

17. (Previously Presented) The method as recited in claim 16 wherein the authentication token of the one signal transmitted at the i-th position is a bit-by-bit XOR link or an equivalent logic link of the coding of all the previously transmitted signals and the coding of the respective position in the transmission sequence.

18. (Previously Presented) The method as recited in claim 11 wherein the at least one cryptographic algorithm includes a block cipher.

19. (Previously Presented) The method as recited in claim 18 wherein the block cipher includes a data encryption standard.

20. (Previously Presented) The method as recited in claim 12 wherein the at least one cryptographic algorithm includes a block cipher, the pseudo-random sequence being generated by operating the block cipher in a known output feedback mode.

21. (Previously Presented) The method as recited in claim 15 wherein the at least one cryptographic algorithm includes a block cipher, the pseudo-random sequence being generated by operating the block cipher in a known output feedback mode.

22. (Previously Presented) The method as recited in claim 11 wherein the communication phase further includes calculating another token for authentication of the transmitter, the

other token being subsequently transmitted so as to initialize the receiver for authentication of the transmitter.

23. (Previously Presented) The method as recited in claim 11 further comprising confirming the transmission sequences by nonintersecting m-bit strings.

24. (Currently Amended) A method for transmitting signals between a transmitter and a receiver, the method comprising:

calculating data as a function of a secret key using at least one cryptographic algorithm in a calculation phase, the calculation phase including generating a pseudo-random sequence, certain strings of the pseudo-random sequence being used for coding the signals and positions in the transmission sequence, and wherein the authentication token of one of the signals transmitted at an i-th position is calculated as a function of the coding of the signal and the coding of the respective position in the transmission sequence; and

calculating authentication tokens for the signals as a function of the data in a communication phase so as to authenticate both the signals and a transmission sequence of the signals, the authentication token of the one signal transmitted at the i-th position being a bit-by-bit XOR link or an equivalent logic function of the coding of the one signal and the coding of the respective position in the transmission sequence;

wherein the signals received by the receiver from the transmitter are accepted as authentic if a transmitted authentication token that is received by the receiver matches the authentication token calculated by the receiver.

25. (Previously Presented) The method as recited in claim 24 wherein certain strings of the pseudo-random sequence are used for coding the signals and positions in the transmission sequence, and wherein the authentication token of a one of the signals transmitted at an i-th position is calculated as a function of the coding of all previously transmitted signals and the coding of the respective position in the transmission sequence.

26. (Previously Presented) The method as recited in claim 25 wherein the authentication token of the one signal transmitted at the i-th position is a bit-by-bit XOR link or an

equivalent logic link of the coding of all the previously transmitted signals and the coding of the respective position in the transmission sequence.

27. (Previously Presented) The method as recited in claim 24 wherein the at least one cryptographic algorithm includes a block cipher, the block cipher including a data encryption standard.

28. (Previously Presented) The method as recited in claim 24 wherein the at least one cryptographic algorithm includes a block cipher, the pseudo-random sequence being generated by operating the block cipher in a known output feedback mode.

29. (Previously Presented) The method as recited in claim 24 wherein the communication phase further includes calculating another token for authentication of the transmitter, the other token being subsequently transmitted so as to initialize the receiver for authentication of the transmitter.

30. (Currently Amended) A method for transmitting signals between a transmitter and a receiver, the method comprising:

calculating data as a function of a secret key using at least one cryptographic algorithm in a calculation phase, the calculation phase including generating a pseudo-random sequence, certain strings of the pseudo-random sequence being used for coding the signals and positions in the transmission sequence, and wherein the authentication token of one of the signals transmitted at an i-th position is calculated as a function of the coding of the signal and the coding of the respective position in the transmission sequence; and

calculating authentication tokens for the signals as a function of the data in a communication phase so as to authenticate both the signals and a transmission sequence of the signals, the authentication token of the one signal transmitted at the i-th position being a bit-by-bit XOR link or an equivalent logic function of the coding of the one signal and the coding of the respective position in the transmission sequence; and

confirming the transmission sequences by nonintersecting m-bit strings;

wherein the signals received by the receiver from the transmitter are accepted as authentic if a transmitted authentication token that is received by the receiver matches the authentication token calculated by the receiver.